



# SRC Cyber Security Update



Cobus Nel & Steve Smith



**We're for New Zealand.**  
Tū mai Aotearoa.

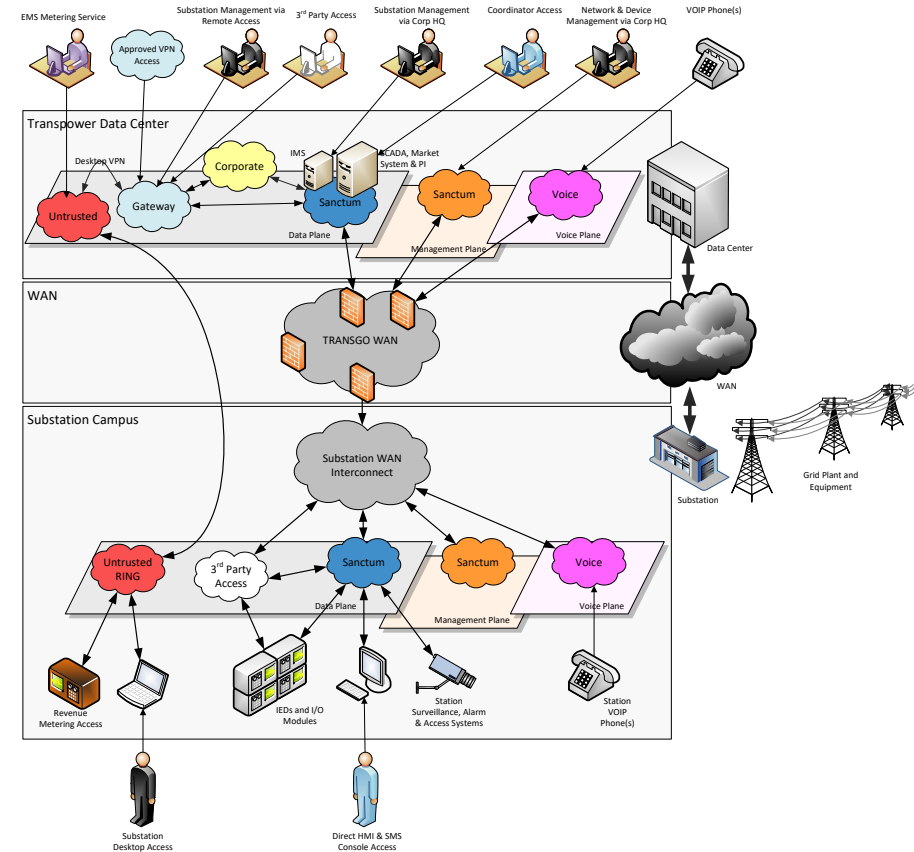
# Content

- Security overview
- Areas of focus (recent, current and near future)
- Our expectations of industry
- Initiatives
- Ventia Event
- GridEx

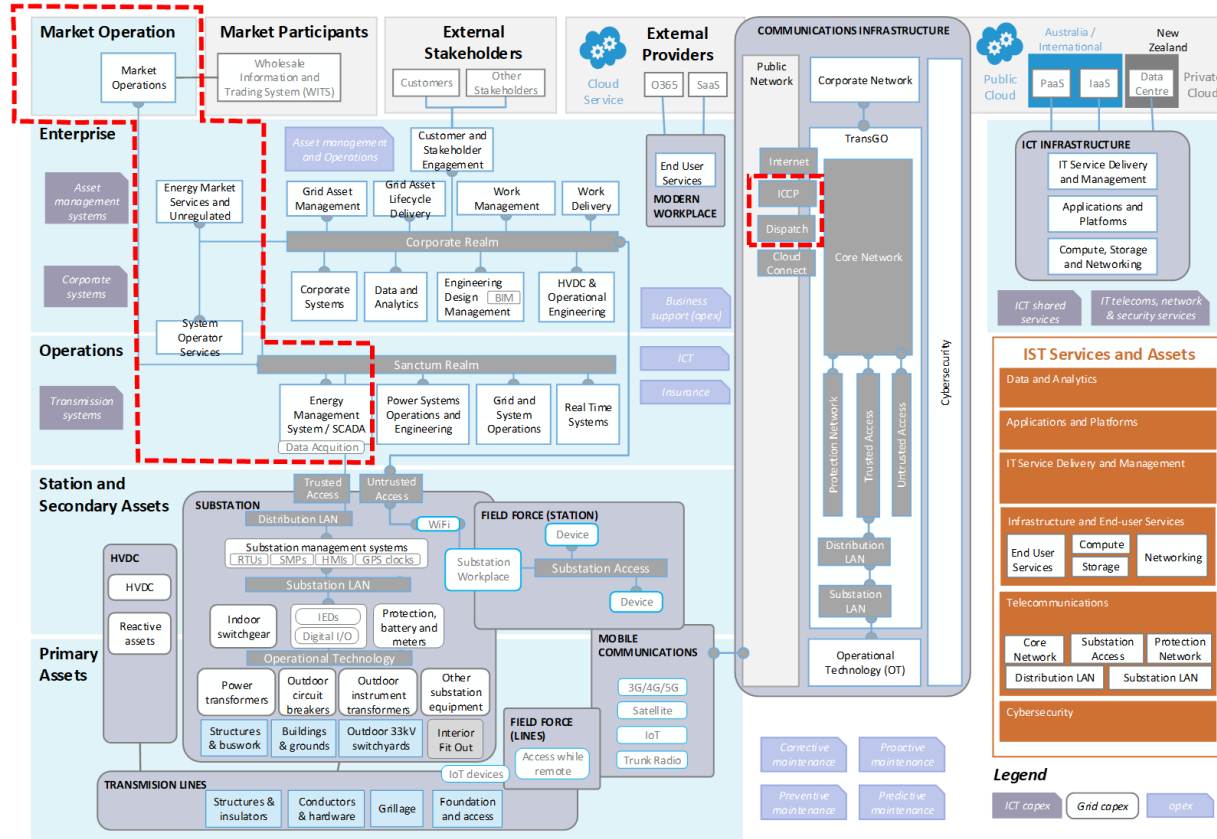


# Security Overview

- Segregation is one of our main controls. There is a hard shell from the sanctum realm externally via corporate, secured through firewalls.
- Sanctum is split into:
  - Substation environment
  - SCADA/Market System environment
- Regionally located virtual firewalls secure substation services.
- Planes and realms are utilised to ensure further segregation and traffic management.
- Multi-factor authentication is used to gain access to Corporate and again (separate) into Sanctum.



# Where Market Systems fits in



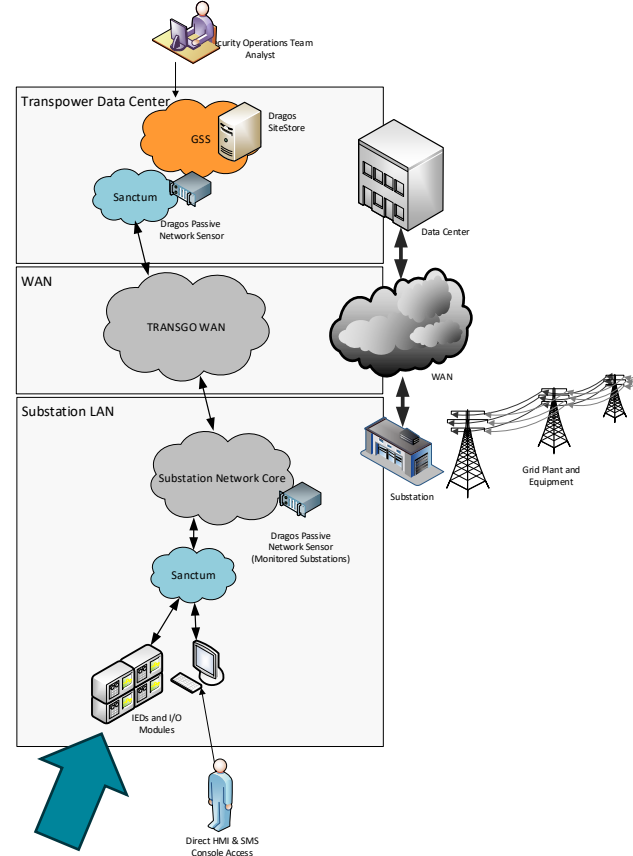
# Focus areas for the last year

- Next stage of Remote Engineering Access to secure our substation environment
- Refreshing our Firewalls (move from Checkpoint to Fortinet)
- Phishing and cyber education
  - Training
  - Tests/exercises
- Introduction of Dragos OT threat/vulnerability detection/management
- Extend the deployment of comprehensive end-point protection to our Linux fleet.



# Substation - Dragos

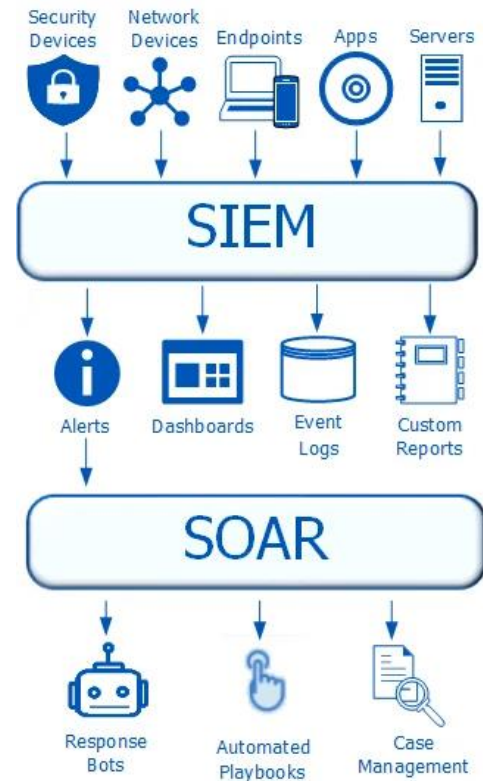
- Our Operational Technologies are our “crown jewels”.
- Protecting these from threats is a combination of managing the hard shell whilst monitoring the softer core.
- Dragos Specialist passive network sensor
  - Scans devices and traffic within the substation
    - Authorised? Normal traffic flow? (internal, operational)
  - Identify OT vulnerabilities and provides recommendations
- Vulnerabilities are managed via responsible divisions for IEDs, SMS and HVDC/reactive equipment held in substation LAN.
- We have Dragos sensors deployed at 6 of our major substations.



IED – Intelligent Electronic Device or relay  
SMS – Substation Management System  
HVDC and Reactive specialist equipment

## Current Focus Areas

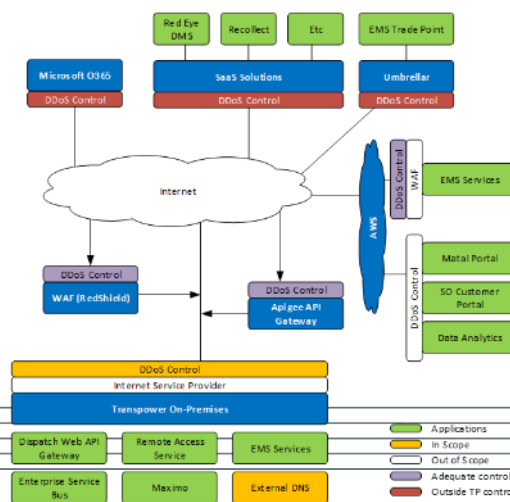
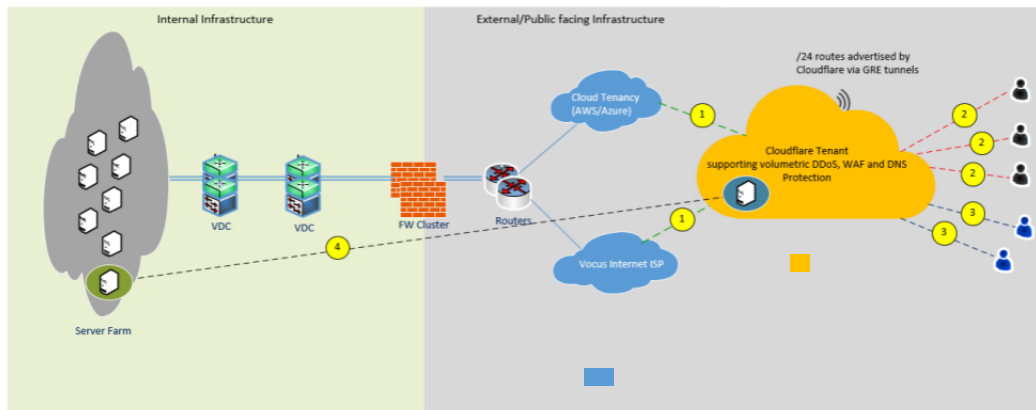
- SIEM/SOAR (Operational Threat Platform)
  - Modernise our platform (we currently utilise Logarithm)
- DDoS/DNS
  - We have on-shore DDoS protection and looking at enhancing it with off-shore protection.
- Continuation of Identity and Access Management roadmap and improvements
- Tenancy uplift and review of our cloud infrastructure
  - Ensure our cloud tenancies are scalable while complying with our security architecture and standards (AWS and Azure).





# Current focus areas - DDOS/DNS

- We currently have adequate coverage for most probable attack
  - ISP coverage for infrastructure
  - Redshield Dispatch/EMS tradeport
  - Cloud native for Azure/AWS
- To move to best practice protection against our most likely worst-case scenario for all these areas, move to an industry leading cloud-based DDoS and DNS hosting.
- This will enable:
  - Faster time to mitigate
  - Larger scrubbing capability (off-shore)
  - Independence from service provider.



# Future focus areas

- Firewalls
  - Moving from regionally located virtual firewalls to firewalls at the substation as part of our TransGO refresh programme. Improved security and control as a result.
- Identity and Access Management
  - Leverage the benefits of cloud-based identity management and “federation” while still maintaining the ability to function in a black start scenario when the cloud is not available.
- Advanced phishing management and culture/competency assurance
- Automated penetration testing
  - Evaluate the benefits from automated penetration testing to assist in prioritising vulnerability management interventions.



Keeping ahead



# Where we look to others



National Cyber  
Security Centre  
a part of GCHQ



- The NZ Energy Industry is small and often have overlapping providers and threats. Relationships are important.
- CSSIE – Control Systems Security Information Exchange
  - Is an important forum to exchange and grow cyber capability and maturity with alignment. It is important this is encouraged and supported with openness.
    - Methods to connect in case of events/incidents and share without risk is an ongoing conversation.
    - Sharing learnings and areas of focus.
- Our connection to CERT NZ and NCSC is important and hopefully growing
- Grow our talent pool
  - Resource is in demand and is going to increase, we all need to do our part to invest in the NZ security capability



# Initiative Suggestions

- Support CSSIE participation and sharing activities
- Support distributed participation / planning of GridEx
- Participation in ICSJWG (US) and NZ ICS Cyber Technical Network\*  
ISAC cyber "capture the flag"
- How do we interconnect/interact with each other as an industry in a standardised and secure manner? How does industry assure itself? Position/exposure with DER expansion in NZ?



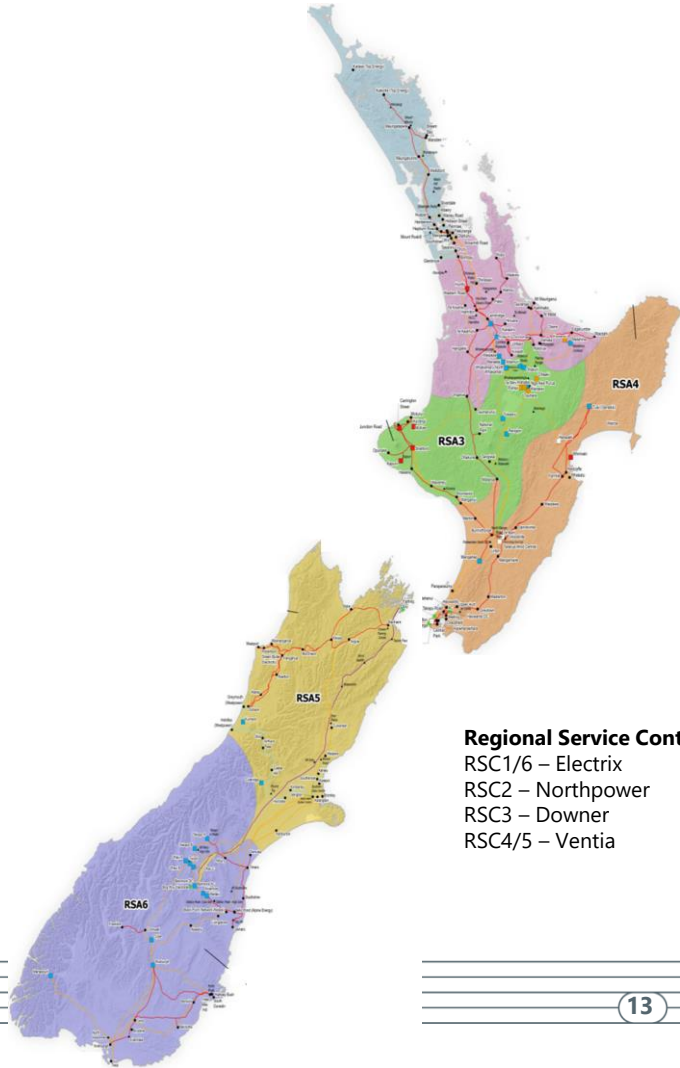
CISA INDUSTRIAL CONTROL  
SYSTEMS JOINT WORKING GROUP

NZ ICS  
CYBER  
TECHNICAL  
NETWORK

\*some good uptake in industry

# Ventia Event

- Ventia are a service provider for Transpower and deliver fieldworks in the form of:
  - Proactive and planned maintenance/switching
  - Fault response and event support (e.g. Gabrielle)
  - Project delivery
- Our service providers are very “hands on” in all ways:
  - Connect and configure our protection equipment in substations, handle primary equipment in field, wire and configure substation communication hardware and software.
- Ventia cover regions RSA4 and RSA5 and Telecommunications nationally.

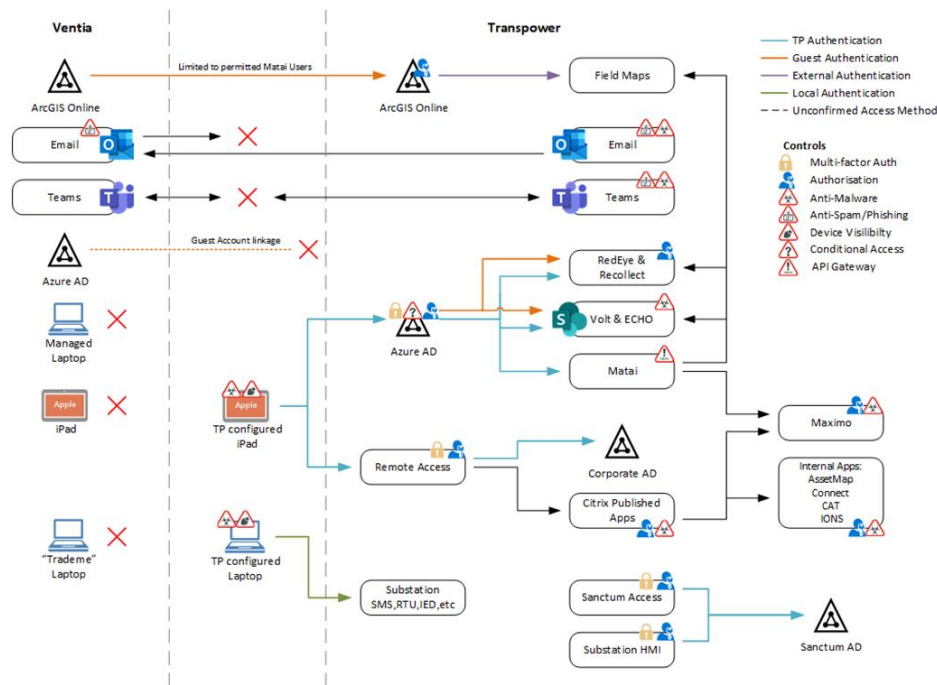


## Regional Service Contracts

RSC1/6 – Electrix  
RSC2 – Northpower  
RSC3 – Downer  
RSC4/5 – Ventia

# Ventia Access

- Ventia utilise Transpower systems using their laptops.
- The diagram depicts the various connections to Transpower systems and the disconnections during our response
- Potential risks to Transpower were via Ventia's laptops either at our substation or through "guest" or remote access connections.



# Ventia Event - Overview

## The background

- A legacy archived server was re-livened into the Ventia environment in conjunction with a managed service provider. This was done to access historical data.
- The server (due to its age) was an old build and unpatched. This resulted in vulnerabilities which combined with exposure to the internet resulted in compromise via a threat actor.
- After a period, the threat actor attempted to move laterally from the server into other targets using local and service accounts harvested. Moves were blocked by Protection installed in the “new environment”.
- Data was exfiltrated from the old environment on the 3<sup>rd</sup> of July to threat actor-controlled infrastructure. This information did not include any information pertaining to Transpower (predated the Transpower contract).
- The threat actor attempting to connect to and integrated lights out interface (iLO) on the 4<sup>th</sup> July triggered further investigation which was completed on the 5<sup>th</sup> of July.
- An increase in malicious incoming spam e-mail was observed by Ventia staff on the 7<sup>th</sup> July and Ventia declared a critical incident informing Transpower late evening on the same day.
- Transpower's connections and identities for Ventia were all disabled immediately on notification.



# Ventia Event Response

- No evidence of compromise within Transpower.
- We treated it as a Major event - (full incident response structure created across GMT, IST and Grid Delivery).
- Immediate disconnection from Ventia was successful and justified.
- Transpower BCP immediately kicked in with Grid IMT – collaboration and IMT interconnection was strong.
- “Fog of war” was an issue with often conflicting messages. This is usually the case in events of this nature.
- Restoration was systematic and supported through third party assurance (PWC) for each step.
- We are working with PWC to capture lessons learnt and validate:
  - Ventia’s arrangements, interconnectivity and risks imposed
  - Transpower’s controls
- We are confident that the event did not pose any threat to us, there however is always learning both from our controls and the business continuity and response process.





# GridEx

- On 14<sup>th</sup> and 15<sup>th</sup> November 2023 the North American Electric Reliability Corporation (NERC) will hold their biennial grid security exercise. The intention is for utilities to demonstrate how they would respond to and recover from simulated cyber and physical security threats and incidents and to strengthen their crisis communications relationships.
- Transpower has participated in the exercise since 2019 and matured the approach through GridEx V (2019) and VI (2021).
- This year's event will take a similar form to the previous exercises, and we have incorporated the lessons learnt from the past.
- Prior to starting the planning, feedback was requested from participants in/observers of GridEx VI. The feedback included:
  - Positive feedback on learnings and engagement from several participants.
  - A challenge relating to lack of understanding of the current state of the grid at various stages during the exercise (e.g. GXP outage or not, transmission constraints etc.)
  - Preference for a greater focus on cyber impacts within the scenario.



# GridEx Cont..

In response to the feedback:

- We will share the scenario with external participants so they can develop organisation specific scenario planning. This will enable participants to build into their scenarios specific aspects they want to focus on.
- We will also increase the utilisation of maps to assist with conveying current state Grid/system state for the moves/injects.

Participants will not modify the overarching Transpower scenario as a part of development but should be significantly more engaged and able to support the event during the exercise.

The development of material has commenced with the receipt of the NERC originals. The overall Scenario has been assessed and converted to New Zealand context. Content follows the normal pattern of the exercise as follows:

- Move 0: Introduction into the scene for the nation – conditions, culture, precursors etc..
- Move 1: Initial events with aspects of all areas of security
- Move 2: Escalation of these to increase the impact to Transpower and connected parties
- Move 3: Move to country wide crisis management.
- Move 4: Final escalations and fundamental breakdown



## GridEx Cont..

- The Authority have people involved in the two days as observers.
- The core team developing and delivering the exercise is as follows:
  - Steve Smith – Sponsor, facilitator on the day (IST)
  - Peter Gillam – Lead material developer, timeline and moves/injects on the day (IST)
  - James Hurley – NCSC material development support (NCSC)
  - Andrew Renton – Context and material support for grid (Grid Development)
  - Karen Sinclair – Project Management - schedule/coordination support (Grid Development)
  - Jonathan Pawley – NCSC lead and acting the role of NCSC on the day (NCSC)
  - Sam Leggett – CERT lead (CERT)
  - Alice Boraston – Police lead and acting the role of Police on the day
  - TBC – DPMC lead and acting the role for whole of Government on the day
  - Multiple – Authority observers



# Questions?

